Mr. Preston Marshall
Program Manager
Advanced Technology Office

Robust Tactical Networks

We are now going to discuss the exciting part, the technology needed to connect the fast moving aircraft, people, vehicles, robots, sensors, and all the devices of the modern military, into one seamless network

Why is wireless networking so important? According to the Secretary of Defense, our military strategy is to achieve full spectrum dominance using decentralized execution and decision superiority. Decentralized execution organizes and executes at increasingly lower echelons. These echelons are, by nature, mobile, and, therefore must be independent of the fixed infrastructure. They must be wireless. Full spectrum dominance is the ability to "sense, understand, decide, and act faster than any adversary, in any situation." This means that our networks must not just be wireless, they must be fast, reliable in all situations, and integrated.

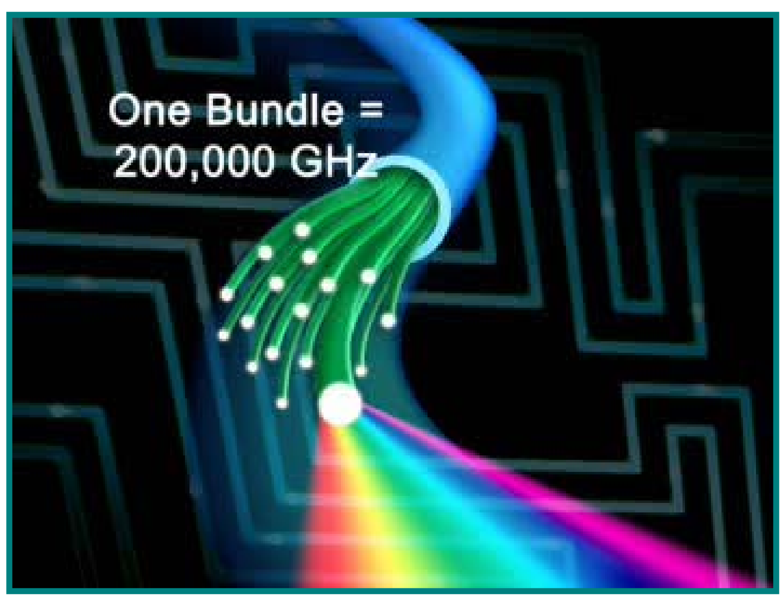
Again, in the words of the Secretary, "this requires a singular battlespace, networked to enable continuous and collaborative campaign planning." The weapons are not just in the platforms; the network itself may be our greatest weapon!

For the next 10 minutes, I will talk about how DARPA is going to help create the network-centric technology to meet his extreme challenge. Our vision is of a seamless network connecting all battlefield assets. An integrated network that is its own infrastructure, and inherently expands as we deploy more of our forces. Wireless devices dynamically connect to any node, find routes, optimize their individual technologies, locate spectrum, create trust, and adapt as needs change. Quite a challenge!

We do not want our soldiers to think about, or even know that this link was on VHF terrestrial radio, or that this one was a UHF Mobile Network. In the past we attempted to build the best radio, now we have to transition our thinking to what is the best wireless network. This is the DARPA challenge.

One reason commercial wired technology has been successful, has been a clean separation between the technology layers of the network. In the wireless space, we need to do the opposite: fuse and integrate these functions so that they can optimize not only themselves, but each other.

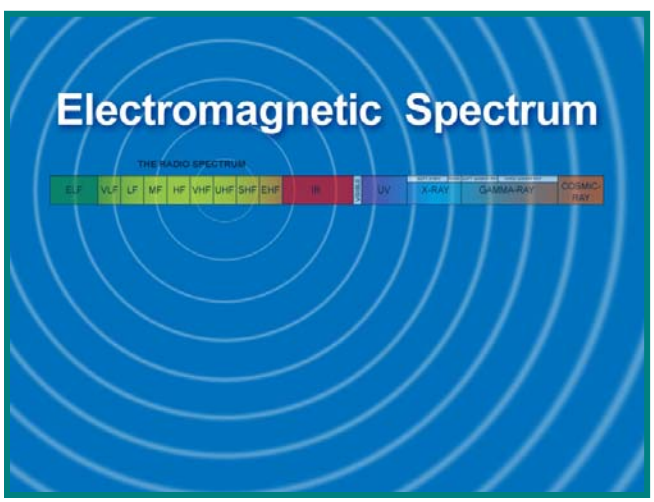
For a while, some believed this vision could be achieved by porting the successful Internet technology to wireless. As we research this, it becomes clear that this is not a sufficient approach. For one, Internet technology is based on scalable media. If you want more bandwidth, you just buy another hub. With multiplexing, a single 20-fiber bundle can theoretically carry 200,000 gigahertz of analog bandwidth. By contrast, we typically have less than three gigahertz for wireless users, and the



Robust Tactical Networks

DoD has access to only several hundred megahertz for all of its mobile devices. The spectrum for mobile devices is just over 0.001 percent of what one fiber bundle can carry. How can we reconcile technology based on unconstrained scalability to one with a zerosum constraint on use?

Commercial wireless technologies are generally based on towers and high-power base stations. They are fixed in location and relationship to their client devices. These are clearly not an option for DoD. As we build a technology base for future military networks, we must address the reality that communicating close to the ground is quite simply a hard, tough problem. Terrain blocks signals. Rapid topology changes would flood a conventional network. Internet protocols can consume one hundred times the bandwidth of the information being sent. And, the military is not alone in looking to the wireless spectrum. In this room, I would guess that there are over 1,000 cellphones, 500 blackberries, and hundreds of laptop WiFi cards. Worldwide, we get a small, and likely diminishing, portion of this RF spectrum. Lastly, even though communications technology is becoming increasingly digital, often it is the limitations of the analog technology that constrain us. Our demand for information is growing faster than analog to digital converter speed is increasing. While commercial wireless devices often can use limited performance receivers, we must operate military systems in the presence of large numbers of high-power signals. New waveforms are advantageous, but force us to use amplifiers with one quarter the efficiency.



In many areas, we can look to commercial technology. But in wireless networking, DoD is on its own. Previous research by DARPA has established the basic framework of future networking, through programs such as Global Mobile Information Systems (GLOMO), which developed packet radio networks, SpeakEasy, which was the first Software Defined Radio, and SUO, which demonstrated self-forming, tactical networking. Our current programs have the potential to revolutionize many aspects of military wireless networking. Next-generation communications will opportunistically exploit unused spectrum without interfering with other spectrum users, yielding a ten-fold increase in the capacity of our systems.

Connectionless Networking will reduce energy usage for sensor networks by a factor of 100. Disruption Tolerant Networking will enable use of networks that have only intermittent connectivity. MnM will extend multiple input/multiple output (MIMO) technology to mobile platforms, increasing the number of users by a factor of at least five. Dynamic Optical Tags and Optical and RF Combined Link Experiment (ORCLE), are both moving wireless communications out of the RF spectrum entirely, leading to wireless networks that approach fiber speeds.

Even with the work underway, we are still short of the technology needed to achieve this vision. I would like to point to some specific technology ideas we have, and where we need your help.

First, how do we operate networks where the number of devices is extremely large and so dynamic that we cannot maintain and distribute topology information? ARPANet originally connected universities, then workstations, then offices and homes, and now people. Soon it will connect the individual devices we depend upon. For our soldiers this means each weapon, sensor, remote sensor, supply and so on. There are a little over five million dot coms in the Internet. Compare that to the total number of devices DoD owns.

The legacy network topologies are fixed, while we envision constant change. By the time the network updates its routing, the routes may have all changed! Having complete and current topology awareness will be a luxury for our future military networks! We have started research in partially aware networks, but much more remains to be done!

Second, how do we manage the option space our technology is making available? As we increase the number of devices, we increase the number of routes, waveforms, and spectrum options we must consider. As we build software radios, we increase the number of waveforms a radio can employ. How do we decide the best way to operate, when the alternative space is essentially infinite and constantly changing? How do we consider the effect of our decision on all of the other members of the network?

Let's consider one example. Internet routing uses the shortest path, pretty common sense. Let's think about a mobile, terrestrial network when a helicopter flies over. Logically, we want the helicopter link to be used only for traffic that has no other delivery path. However, suddenly the helicopter is perceived by all nodes as the shortest path to every other node, immediately becoming saturated, ending up actually degrading the network! This is one simple example, but what is the generalized technology that we can develop to make the hundreds of similar, but less obvious, decisions that are needed every second?

Consider how many IT people it takes to support fixed enterprise networks. Then, imagine if we apply these same ratios to future military networks. We need automatic topology organization, management, and problem solving to make network operation as inherent as in appliance. We are looking to apply reasoning and cognitive technology to these decisions, but again, this investigation is just in its infancy.

Third, today networks share common algorithms, protocols, and information exchange models. Our military networks range from small, battery-powered wireless devices to large command centers. It is hard to believe that what is right at the command center, is right for the battery-dependent device. We need local adaptation.

Such a network would enable each level, region, and application to use different operating rules, principles, routing algorithms, and so on. As you move through such a network, rules at each node adapt to the needs of neighboring nodes. How can we describe such processes, ensure they are stable at the boundaries, and capable of dynamic integration? The number of conditions, states, interactions, and the rate of change, appears too high to be supported by conventional programming logic. In current and future programs, we are looking to isolate the algorithms from the network's interoperability so that we can extend and adapt the key network mechanisms on a local level.

Fourth, and perhaps most significantly, we need to look beyond our current thinking of networking and the Internet protocol assumptions that have become almost laws of science. Today, the packet network layer is the basis for all of our Internet technology. It has served us well for non-real-time applications. However, increasingly, we need to migrate time-critical streaming services, such as voice, video and conferencing, to our integrated networks. In the fixed Internet, this inherent conflict is addressed by over-provisioning of bandwidth to achieve quality of service, an approach that is not applicable to the wireless edge.

In ATO, we think we need a network model that is designed for these streaming and broadcast services. This model should not be a discrete or disjoint alternative to the current IP network, but instead, one that can coexist with it, sharing resources such as routers and the underlying communications network. Imagine if we could have multiple network technologies simultaneously; IP version four and six and a stream-oriented Disruption Tolerant Network layer all sharing the same physical resources. We would have the ability to evolve network technology and match technology to needs throughout our vast GIG without the disruption of wholesale technology migration.

The migration to the latest IP version will take longer to accomplish than the original build out of the Internet! We cannot develop and deploy enhanced technology if we can not find more responsive ways to exploit it. There are opportunities that we can only exploit if we can break out of the mindset of one successful technology in order to develop the next.

Lastly, the military environment we want to support is changing dramatically. Classically, military communications have been vertical. Information flows upwards through echelons, and command and control direction flows downward. Soldiers have low bandwidth voice radios; upper tier command centers have fast ones.

The enterprise model is history. In the future, the lower tactical layer will become richer in information, access and fuse sensors directly, control robotic and other devices, and pull information from upper layers. Importantly it will be rich in collaboration within the tactical level.

Our challenge is how to integrate these two very different network needs. The network must allow information at the tactical layer to flow both vertically and laterally to support all levels of decision making. We need an hourglass, not an inverted pyramid.

The technologies we seek to develop are not individual or standalone. All provide our networks the ability to adapt to environments and military needs. Our radio vision is a cluster of RF components. Where there is no spectrum, we use dynamic spectrum to find holes. Where there are no spectrum holes, or too much multipath, we exploit MIMO technology. When we get interference, we use dynamic spectrum to find new frequencies, or our MIMO resources to null it. When service quality is threatened, we reconfigure the topology. When we are short of energy, we behave like a connectionless network

Many of the technologies we have discussed are too important to wait for new acquisition programs. We seek to integrate them into ongoing acquisition so the warfighters get immediate benefit. We are working with the acquisition community so systems being acquired can host these new DARPA technologies as we develop them.

Many of the technology underpinnings of network-centric warfare originated in DARPA programs over a decade ago. Even a decade later, this vision is far from complete. We want your ideas on how to complete the vision.